

Return

Case No.:

Date and time warrant executed:

Copy of warrant and inventory left with:

Inventory made in the presence of :

Inventory of the property taken and name(s) of any person(s) seized:

Certification

I declare under penalty of perjury that this inventory is correct and was returned along with the original warrant to the designated judge.

Date: _____

Executing officer's signature

Printed name and title

ATTACHMENT A

Property to Be Searched

This warrant applies to GPS location data for all records and unique device/user identifiers pertaining to location information during the following listed date and times,

1. Device #1:

IMEI #350182015213236 belonging to 2023 Toyota Camry bearing VIN

#4T1G11AK4PU760822, on April 27, 2024, from 3:00 AM until 7:20 AM.

ATTACHMENT B

Particular Things to be Seized

I. Information to be Disclosed by the Provider

To the extent that the information described in Attachment A is within the possession, custody, or control of Toyota Motor Sales, USA and Toyota Motor North America, Inc., including any information that has been deleted but is still available to the Provider or that has been preserved pursuant to a request made under 18 U.S.C. § 2703(f), the Provider is required to disclose to the government the following information pertaining to the Account listed in Attachment A for the time period of April 27, 2024, from 3:00 AM until 7:20 AM:

- a. The following information about the customers or subscribers of the Account:
 - i. Account Names (including subscriber names, usernames, and screen names);
 - ii. Addresses (including mailing addresses, residential addresses, business addresses, and e-mail addresses);
 - iii. GPS locations of the vehicle;
 - iv. Other subscriber numbers or identities (including the registration Internet Protocol (“IP”) address);
 - v. Means and source of payment for such service (including any credit card or bank account number) and billing records;
- b. All records and other information (not including the contents of communications) relating to wire and electronic communications sent or received by the Account, including:
 - i. MMS, and data; email addresses and IP addresses (including source and destination); websites visited;
 - i. IMEI/IMSI, or other device identifiers of devices connected to the onboard “connected services” of the vehicle;

- ii. All historical text content available pursuant to this warrant.
- iii. Data obtained by Toyota which is collected from devices which connect to the onboard “connected services” of the vehicle, including text, email, contact lists, phone numbers, IMSI/IMEI numbers, IP addresses, advertising ID numbers, social media accounts.

II. Information to be Seized by the Government

All information described above in Section I that constitutes evidence, fruits, contraband, and instrumentalities of violations of Title 18 U.S.C. §§ 2119(1) (Carjacking) and 924(c) (Brandishing of a Firearm during a Crime of Violence).

Law enforcement personnel (who may include, in addition to law enforcement officers and agents, attorneys for the government, attorney support staff, agency personnel assisting the government in this investigation, and outside technical experts under government control) are authorized to review the records produced by the Provider in order to locate the things particularly described in this Warrant.

for the
Eastern District of Wisconsin

Case No. 24-M-520 (SCD)

Case 2:24-mj-00520-SCD Filed 11/07/24 Page 6 of 16 Document 1

**AFFIDAVIT IN SUPPORT OF
AN APPLICATION FOR A SEARCH WARRANT**

I, Paul Kozelek, being first duly sworn, hereby depose and state as follows:

INTRODUCTION AND AGENT BACKGROUND

1. I make this affidavit in support of an application for a search warrant for records and information associated with certain “connected cars” that are in the possession, custody, and/or control of the following company(s): Toyota Motor Sales, USA and Toyota Motor North America, Inc. (here in, Toyota) whose representative is CT Corporation located at 301 South Bedford Street, Madison, WI 53703. The information to be searched is described in the following paragraphs and in Attachment A. This affidavit is made in support of an application for a search warrant under 18 U.S.C. § 2703(c)(1)(A) to require Toyota to disclose to the government copies of the information further described in Attachment B.

2. I am a Special Agent with the Bureau of Alcohol, Tobacco, Firearms and Explosives (ATF), and have been since January of 2020. Prior to my employment with ATF, I was a Sheriff’s Deputy with the Jackson County Sheriff’s Office in Black River Falls, WI. My duties included patrol, drafting and executing search warrants, and investigations related to state and county criminal violations. Previous to my tenure with the Jackson County Sheriff’s Office, I served with the United State Marine Corps from 2004 until 2008, and the United States Marine Corps Reserve from 2011 until 2014. I left the Marine Corps as an E6/Staff Sergeant holding the billet of Platoon Commander. I received my bachelor’s degree in Criminal Justice Administration from Viterbo University, La Crosse, WI in 2016.

3. I have completed approximately 26 weeks of training at the Federal Law Enforcement Training Center in Glyncro, Georgia, as well as the ATF National Academy. That training included various legal courses related to constitutional law as well as search and seizure

authority. Additionally, I have received training on how to conduct various tasks associated with criminal investigations, such as interviewing, surveillance, and evidence collection.

4. I have previously applied for and received search warrants related to cell site data and other related cellphone company records.

5. This affidavit is based upon my personal knowledge as well as information provided to me by other federal, state, and local law enforcement officers during the course of their official duties, all of whom I believe to be truthful and reliable. This affidavit is also based upon information gathered from interviews of citizen witnesses, reports, official records, law enforcement reports, and my training and experience.

6. Based on the facts set forth in this affidavit, there is probable cause to believe that violations of Title 18 U.S.C. §§ 2119 (motor vehicle robbery/carjacking) and 924(c) (brandishing a firearm during a crime of violence) have been committed by multiple unknown individuals. There is also probable cause to search the information described in Attachment A for evidence of these crimes as further described in Attachment B.

PROBABLE CAUSE

7. Your Affiant reviewed Milwaukee Police Department report #C2404270032. Your affiant is aware that on April 27, 2024, at approximately 4:00 AM the victim identified as A.W. (F/B DOB XX/XX/1999) left her place of work at the Potawatomi Casino located at 1721 W. Canal St. in the City of Milwaukee. A.W. drove to her residence and parked in front of 2298 W. Kilbourn Ave. at approximately 4:06 AM. A.W. told police she fell asleep in the driver seat of her vehicle. At 5:00 AM, she was awoken by Suspect 1 and Suspect 2 opening the doors of her vehicle. A.W. stated a black male wearing a facemask and holding a handgun demanded she exit the vehicle, while Suspect 2 opened the rear passenger door, also masked and holding a handgun.

A.W. exited her vehicle and Suspect 1 entered the driver seat while Suspect 2 entered the front passenger seat and drove off with the vehicle. A.W. immediately called police to report the incident.

8. The vehicle was described as a 2023 Toyota Camry, silver in color bearing Wyoming license plate 019219, VIN #4T1G11AK4PU760822 (Device 1). This vehicle was rented from Enterprise Rent-A-Car. A.W. contacted Enterprise and was given location information for the vehicle. At 7:20 AM officers were notified the vehicle was parked behind 4801 W. Hampton Ave. in Milwaukee. This address is a 12-unit apartment building. Officers arrived and located the vehicle parked in the rear parking lot for the building. Officers canvased the apartment building and spoke with several tenants. As officers were outside the building, they could hear a male and female inside of apartment one through an open window. When officers tried to get their attention to open the locked outer door to the building, they shut the window. When officers did get inside, they knocked on apartment one whose door was partially open. A female with bright pink hair answered but the male told her to close the door. A few minutes later the male and female exited apartment one and officers approached. The male denied knowing about the stolen vehicle and did not have any information, then the two quickly left.

9. Later, as the vehicle was being towed, a female who identified herself to officers as T.S. (F/B DOB XX/XX/1973) asked why the vehicle was being towed and stated “they just moved in.” Upon questioning T.S. stated at about 7:00 AM that morning she was in the parking lot and saw the male exit the driver seat and female “with pink hair” exit the passenger seat of the vehicle. Officers showed body camera footage to T.S. who confirmed it was the male and female from apartment one.

10. The vehicle was processed by Milwaukee Police Department (MPD) and three latent prints were lifted. One of these prints was a palm print from the exterior of the passenger side rear window. This matched to Anthony T. TATE (M/B DOB XX/XX/2000). A review of TATE's criminal history showed a felony conviction on October 24, 2018, Waukesha Co. case #2018CF001101 for drive/operate vehicle without owner's consent, and on April 21, 2022, Milwaukee Co. case #22020CF002387 robbery with threat of force.

11. On May 28, 2024, a federal subpoena was issued to Toyota Motor North America Inc. seeking the International Mobile Equipment Identity (IMEI) number for the Toyota Camry bearing VIN #4T1G11AK4PU760822. On June 6, 2024, SA Kozelek received a reply from Toyota Motor North America Inc. showing the IMEI number to be 350182015213236. In my training and experience, identifying the location of the stolen vehicle during the time frame of the theft will aid in identifying the identities of Suspect 1 and Suspect 2.

12. In my training and experience, I have learned it is possible to obtain historical location data from certain vehicles based on an onboard cellular device installed in the vehicle. The installed cellular device is assigned two identifiers known as the International Mobile Equipment Identity (which is analogous to a serial number assigned to the device and abbreviated "IMEI") and an International Mobile Subscriber Identity (which is assigned to a subscriber and abbreviated "IMSI"). Your affiant knows that vehicle manufacturers maintain records regarding the IMEI/IMSI numbers associated with each vehicle equipped with a cellular modem, and that if a vehicle identification number (VIN) is provided to the manufacturer, the IMEI/IMSI numbers associated with that particular device and vehicle can be obtained from the manufacturer. These identifiers allow the cellular device in the vehicle access to a cellular network and once connected to the network, the device can send and receive data across the cellular network.

13. Manufacturers often use this data connection for vehicle performance monitoring, sending software updates to the vehicle, and to enrich the user experience by providing a “wifi hotspot” which connected users can access online content. This cellular device operates like a cellular phone on the cellular providers network and the network creates and maintains records for the device which can include the date and time of connections, the tower and sector that provided the connections, and specialized location data. Once the IMEI/IMSI number is identified, records containing the location data associated with the cellular device in the vehicle can be sought from the cellular provider. These records would allow your affiant to geolocate the location of the vehicle at times relevant to the investigation.

14. In many instances, the manufacturer, in addition to any cellular service to the vehicle, can utilize GPS positioning to provide navigation services (i.e., maps and directions), “find my car” services, and stolen vehicle recovery. The manufacturers collect and retain this information for a period of time depending on a variety of factors, including whether or not the vehicle owner subscribes to certain services. In this instance, Toyota offers “connected services” which include “Safety Connect” which is an Emergency Assistance Button, Enhanced Roadside Assistance, Automatic Collision Notification, and a Stolen Vehicle Locator. Another service is “Service Connect” which includes Vehicle Health Reports, Vehicle Maintenance Alerts, and Maintenance Reminders. It allows up-to-date information on the health and status of the vehicle. Another service is called “Drive Connect” which allows access to real-time traffic elements, 24/7 live agents and voice commands. It allows access to features on the Cloud as well as live agents can help drivers get to their destination. A fourth service is called “Remote Connect” and allows a vehicle owner to start, lock/unlock doors, using a smart device including a smart watch. A last service is called “Wi-Fi Connect” which connects the vehicle to cell tower services provided by

AT&T. This service connects up to five devices using 4G LTE technology (as of 2024). Also available on select 2022 and later Toyota vehicles, is Integrated Streaming which allows users to connect existing Apple Music and/or Amazon Music subscription through the onboard Audio Source feature.

15. These features all rely on GPS positioning as well as a cellular connection, and with the vehicle identification number, Toyota can provide the historical records for the vehicle at a given date/time.

16. These services, both the cellular connection and GPS positioning, are based on services to which the vehicle owner subscribes. A subscription requires an online account through Toyota and Toyota collects certain information (per their privacy policy) about the subscriber including an account name, account holder/username, date of birth, postal address, email addresses, and driver's license number. Toyota (again per their privacy policy) may also collect information about devices connected to the vehicle to utilize services and/or devices which access the Toyota Connect services application. This information can be important to identify the persons in and around the vehicle.

17. Thus, the records described in Attachment A will identify the location of the following device:

- a. 2023 Toyota Camry bearing VIN #4T1G11AK4PU760822, IMEI #350182015213236 on April 27, 2024, from 3:00 AM until 7:20 AM.

18. Probable cause exists to believe that the records requested contain evidence related to identifying the unknown individuals who committed violations of Title 18 U.S.C. §§ 2119(1) (Carjacking) and 924(c) (brandishing a firearm during a crime of violence).

AUTHORIZATION REQUEST

19. Based on the foregoing, I request that the Court issue the proposed search warrant, pursuant to 18 U.S.C. § 2703 and Federal Rule of Criminal Procedure 41.

20. I further request that the Court direct Toyota Motor Sales, USA and Toyota Motor North America, Inc. whose representative is CT Corporation to disclose to the government any information described in Attachment B that is within its possession, custody, or control. Because the warrant will be served on Toyota who will then compile the requested records at a time convenient to it, reasonable cause exists to permit the execution of the requested warrant at any time in the day or night.

21. I further request that the Court order that all papers in support of this application, including the affidavit and search warrant, be sealed until further order of the Court. These documents discuss an ongoing criminal investigation that is neither public nor known to all of the targets of the investigation. Accordingly, there is good cause to seal these documents because their premature disclosure may seriously jeopardize that investigation, including by giving targets an opportunity to destroy or tamper with evidence, change patterns of behavior, notify confederates, and flee from prosecution.

ATTACHMENT A

Property to Be Searched

This warrant applies to GPS location data for all records and unique device/user identifiers pertaining to location information during the following listed date and times,

1. Device #1:

IMEI #350182015213236 belonging to 2023 Toyota Camry bearing VIN

#4T1G11AK4PU760822, on April 27, 2024, from 3:00 AM until 7:20 AM.

ATTACHMENT B

Particular Things to be Seized

I. Information to be Disclosed by the Provider

To the extent that the information described in Attachment A is within the possession, custody, or control of Toyota Motor Sales, USA and Toyota Motor North America, Inc., including any information that has been deleted but is still available to the Provider or that has been preserved pursuant to a request made under 18 U.S.C. § 2703(f), the Provider is required to disclose to the government the following information pertaining to the Account listed in Attachment A for the time period of April 27, 2024, from 3:00 AM until 7:20 AM:

- a. The following information about the customers or subscribers of the Account:
 - i. Account Names (including subscriber names, usernames, and screen names);
 - ii. Addresses (including mailing addresses, residential addresses, business addresses, and e-mail addresses);
 - iii. GPS locations of the vehicle;
 - iv. Other subscriber numbers or identities (including the registration Internet Protocol (“IP”) address);
 - v. Means and source of payment for such service (including any credit card or bank account number) and billing records;
- b. All records and other information (not including the contents of communications) relating to wire and electronic communications sent or received by the Account, including:
 - i. MMS, and data; email addresses and IP addresses (including source and destination); websites visited;
 - i. IMEI/IMSI, or other device identifiers of devices connected to the onboard “connected services” of the vehicle;

- ii. All historical text content available pursuant to this warrant.
- iii. Data obtained by Toyota which is collected from devices which connect to the onboard “connected services” of the vehicle, including text, email, contact lists, phone numbers, IMSI/IMEI numbers, IP addresses, advertising ID numbers, social media accounts.

II. Information to be Seized by the Government

All information described above in Section I that constitutes evidence, fruits, contraband, and instrumentalities of violations of Title 18 U.S.C. §§ 2119(1) (Carjacking) and 924(c) (Brandishing of a Firearm during a Crime of Violence).

Law enforcement personnel (who may include, in addition to law enforcement officers and agents, attorneys for the government, attorney support staff, agency personnel assisting the government in this investigation, and outside technical experts under government control) are authorized to review the records produced by the Provider in order to locate the things particularly described in this Warrant.